Risk Management Policy

DCA 059/2018	Rev.: 02-27/09/2018	POL-0009-G	PUBLIC

Purpose: To establish guidelines and guidance for the integrated management of all risks which Vale System entities are exposed.

Scope:

- This policy applies to Vale, its wholly owned (100%) subsidiaries and shall be reproduced to its direct and indirect, subsidiaries in Brazil and in other countries, always respecting these companies' constitutional documents and the applicable law. The principles of this Policy should be applied, whenever possible, by other entities in which Vale has equity interest in Brazil and in other countries. This group of entities, for the purposes of this Policy, is called "Vale System".

Principles and Guidelines for Risk Management:

- Support strategic planning, budget and sustainability of Vale System business.
- Strengthen capital structure and asset management of Vale System.
- Strengthen Vale's governance practices, based on lines of defense model.
- Manage risks considering the concepts of ISO 31000 and COSO-ERM.
- Measure and monitor Vale's System risks, on a consolidated basis, considering the effect of diversification, when applicable, of its whole business.
- Assess the impact of new investments, acquisitions and divestitures on Vale's System risk map and risk appetite.
- Adapt Vale's risk appetite to the needs of its growth plan, its strategic planning and its business continuity.

Risk Concept:

- Risk is the effect of uncertainty on the organizational objectives that manifests itself in many ways, with potential impact on all business dimensions.

Integrated Risk Map:

- The Integrated Risk Map is the tool that contains the risks that might affect the organization, being distributed in categories, which include, but are not limited to, strategic, financial, operational, cybernetic and compliance. The map works as a guide to assess the applicability of the risks by different areas and geographies.
- Periodically, at least once a year or when requested, the risks should be evaluated by Vale's Board of Directors, by recommendation of the Executive Board, and may be maintained, reviewed, excluded or included to the Integrated Risk Map.
- The Severity and Probability tables in the "Risk Management" chapter of Planning, Development and Management Standard (NFN-0001) are tools that help to assess risk events and, prioritize their treatment and aim to minimize the subjectivities and standardize the evaluations, making them comparable.
- The severity table is used to assess the progressive severity of impacts in different dimensions including, but not limited to, Financial, Social and Human Rights, Reputational, Environment, Occupational Health and Safety.
- The Probability table is used to statistically estimate the probability of occurrence of an event, as long as it has a rationale that can be audited. In other situations, the risk owner should evaluate the probability of occurrence.
- The combination of impact severity and probability allows the risk event to be plotted in the Risk Matrix, which is a graphical tool that allows comparisons, allowing prioritization for risk treatment.
- In addition, will be carried out an evaluation of the effectiveness of controls (vulnerability) related to a risk event, considering the results of analyzes performed by the lines of defense, such as, but not limited to: peer assessment, assessment by the 2nd line of defense, internal audit issues, external audit recommendations, consultancies, insurance companies or regulatory bodies, when the relevance of the risk justifies its execution.

Risk Appetite:

- Risk appetite represents the amount and type of risk an organization is willing to accept in its pursuit for value. The risk responses must be defined considering the risk appetite, which can be: accept, mitigate, transfer or reject a risk.
- Accept: when no other action is taken to interfere in its magnitude and the risk profile remains the same. This response is appropriate when the corresponding level of risk exposure is within the tolerance limits of the organization.
- Mitigate: when measures are taken to reduce its magnitude. The purpose of this risk response is to change their levels of impact and probability, so they remain within the risk appetite defined by the organization.
- Transfer: when measures are taken to reduce its magnitude by transferring or sharing, in total or in part, the uncertainties. The most common techniques include outsourcing to specialized service providers, the purchase of insurance products and hedge transactions.
- Reject: when measures are taken to remove the risk, which may mean, for example, closing a business unit, not expanding to a new geographic market or selling a productive asset.
- Vale's Board of Directors is responsible to approve the organization's risk appetite, being proposed by Vale's Executive Board, ensuring that risks are integrated into Strategic Planning and reflected into the budget decisions. The risk exposure strategy should be reviewed annually.

Risk Governance Structure:

- Vale has an integrated Risk Governance flow, which represents how revaluations are periodically carried out to ensure the alignment between strategic decisions, performance and definition of risk appetite by the Board of Directors.

1st line of defense

- Consist on the risk owners and process executors of business, project, support and administrative areas. They are directly responsible for identify, evaluate, treat, monitor and manage their risk events in an integrated way. Must maintain the risks within the defined appetite, implement and execute effective preventive and mitigation controls, ensure appropriate definition and execution of action plans and establish corrective actions for the continuous improvement of risk management.
- Must continuously assess the applicability of risks in the Integrated Risk Map to the activities and geographies under their responsibility.
- Should anticipate to the Executive Board and to the Board of Directors the potential impacts that are in the imminence to occur, following the current governance to address the treatment of mapped risks, as well as present the risks under their responsibility to the Executive Risk Committee, the Executive Board, the Board of Directors or to one of its Advisory Committees, whenever necessary.
- Is responsible for establish and implement Crisis Management protocols and Business Continuity plans for the risk events under their responsibility, whenever applicable. For events with significant impacts, drills should be performed in order to verify the efficiency and effectiveness of the Crisis Management protocols. The frequency of the drills should be defined by the 1st line of defense according to the criticality, observing local rules and specific legislation.
- Must meet the guidelines defined by the 2nd line of defense.

2st line of defense

- Corresponds to risk management, internal controls, policies management, legal compliance and other specialist areas. Supervise and support the work of 1st line of defense, providing training and instrumentation for managing the risks. They must identify and monitor new and emerging risks, ensure compliance with laws, regulations, internal norms and promote continuous improvement in risk management.
- The Board of Directors is responsible for define the responsibilities of Governance, Risk and Compliance (GRC) area including, but not limited to:
  - develop and implement policies, methodologies, processes and infrastructure for integrated risk management;
  - report to the Vale's Executive Risk Committee, periodically, the main risks that Vale System is exposed to, within the defined scope, and how those risks are being monitored, controlled and treated;

  - ensure a compliance environment, not only addressing legal issues, but also including the compliance with internal policies and standards;
  - ensure the compliance with risk governance model.
- For specific risks, there are areas such as Environment, Health and Safety, Corporate Integrity and Information Security, which act as a 2nd line of defense specialist, monitoring risks and controls, and ensuring the compliance with external regulations, policies and standards. The definition of which areas in the company will be the 2nd line of defense specialist is delegated to Vale's Executive Risk Committee.
- Based on the Risk Matrix, the Executive Board will define the scope and the operating model of GRC area, considering the combination of severity with probability whose occurrence could jeopardize the achievement of organization's objectives.

3st line of defense

- The 3rd line of defense is composed of areas with total independence from the administration, that is, the Internal Audit and the Ethics and Conduct Office which perform, observing their respective scopes, evaluations, inspections, by the execution of controls test, risk analysis and investigations of allegations, providing exempt assurance, including on the effectiveness of risk management, internal controls and compliance.

General Governance

- The Board of Directors has, for its advisory, committees that, in general, are responsible for (a) monitor risks and financial controls; (b) monitor all operational risks and controls, including Safety, Environment, Health, Social Performance and reputational risks; and (c) supervise risk management, in accordance with the guidelines established by Vale's Board of Directors.
- Vale's Executive Risk Committee, established by Vale's Board of Directors, is the main body of the risk management structure. It is responsible to support the Executive Board in risk analysis and to issue opinions on risk management of Vale's System. It is also responsible to monitor and manage risks, and report them periodically to Vale's Executive Board. It is supported by specific subcommittees, that issue specialist opinions in their respective area of expertise.

General Rules

- Vale's Board of Directors delegates to the Vale's Executive Board the approval for deployment of this Policy into rules and responsibilities for manage and control the risks.